

### REMARKS

Claims 12-21 were pending in this application. The limitations of claims 20 and 21 have been incorporated into independent claim 12. Accordingly, claims 20 and 21 have been cancelled. The preamble of the pending claims has been amended to recite a system instead of a method. The dependent claims have been amended for clarification purposes and to address the Examiner's §112 rejections. No new subject matter is believed to have been added by these amendments. No claims have been added. Therefore, claims 12-19 remain in this application.

#### Specification Objections

Applicants have amended the title to be more descriptive. The title has also been amended to reflect that a system is being claimed.

#### Claim Objections

Claims 12 and 15 stand objected to for informalities. Applicants thank the Examiner for pointing out the necessary corrections. Applicants believe that the above amendments to claims 12 and 15 overcome the Examiner's informality objections. Reconsideration of these objections is respectfully requested.

#### 35 U.S.C. §112 Rejections

Claims 12-21 stand rejected under 35 U.S.C. §112, second paragraph, for indefiniteness and lack of antecedent basis. Applicants have amended the claims containing variables that were not previously defined. These amendments have been made for clarity purposes and are based on the specification, as filed. Applicants believe that the above amendments to claims 12-21 overcome the Examiner's indefiniteness rejections. Reconsideration of these rejections is respectfully requested.

Claim 12 stands rejected under 35 U.S.C. §112, second paragraph, as being incomplete for omitting essential steps, with such omission amounting to a gap between the steps. Applicants have incorporated the limitations of dependent claims 20 and 21 into independent claim 12. These incorporated limitations cover the aspects of encryption and decryption in the context of the variables in steps (a)-(e). Applicants believe that the above

amendments to claim 12 overcome the Examiner's rejection. Reconsideration of this rejection is respectfully requested.

### 35 U.S.C. §101 Rejections

It is asserted that pending claims 12-21 stand rejected under 35 U.S.C. § 101 for being directed to non-statutory subject matter. The Court of Appeals for the Federal Circuit (CAFC) in *In re Bilski* (Fed. Cir. 2008) determined that a claimed process is patent-eligible under § 101 if: (1) it is tied to a particular machine or apparatus, or (2) it transforms a particular article into a different state or thing. Furthermore, the CAFC determined in *In re Comiskey* (Fed. Cir. 2007) that a mental process-type claim must have a technical arts requirement in that it must recite a microprocessor or other computing machine to carry out the mental process. Accordingly, Applicants have amended the claims in the context of a system that includes a computer having a computer readable medium having stored thereon instructions which, when executed by a processor of the computer, causes the processor to perform certain steps. Thus, the amended claims now comport with the requirements for accepted claimed statutory subject matter and Applicants respectfully request withdrawal of the non-statutory subject matter rejection.

### 35 U.S.C. §103 Rejections

Claims 12-21 stand rejected under 35 U.S.C. §103(a) for obviousness based upon the article entitled *Standards for Efficient Cryptography (SEC 1)-Elliptic Curve Cryptography* of Certicom Research, dated September 20, 2000 (hereinafter "the SEC article") in view of U.S. Patent Application Publication No. 2004/0158597 to Ye et al. (hereinafter "the Ye publication"). The Examiner admits that the SEC article does not specifically teach or suggest the scalar multiplication of steps (i)-(iii). Instead, the Examiner asserts that the Ye publication uses scalar multiplication and that the teachings of the SEC article and the Ye publication would be combined by one skilled in the art as both are directed to elliptic encryption systems with the motivation to enhance performance of the system on a 32-bit processor.

The method disclosed in the Ye publication is implemented using polynomial rings, which is different from that of the present invention in which prime order rings is used. The Ye publication is not reasonably pertinent to the particular problem with which an

inventor at the time of conception of the claimed invention would be concerned with due to the different implementations (polynomial rings vs. prime order rings).

As discussed, the present invention is designed and developed using prime order rings. Specifically, Applicants have used a two-level conversion process (i.e., converting the 160 bit integer into a series of powers of  $2^{31}$  and again converting each coefficient into a binary series). During this process, the claimed invention is utilizing a lookup table as well as search optimization methods, as discussed below.

To optimize the scalar multiplication with the points of the elliptic curve, the following steps are used and claimed:

- 1) Converting a large integer (160 bits or greater) into a series of powers of  $2^{31}$

The large integer  $M$  is divided with a value of  $2^{31}$  to obtain a series of values  $m_0, m_1, m_2, \dots, m_n$ , where the value of  $m_n$  lies in  $[0, 2^{31}]$  so that:  $M = m_0(2^{31})^0 + m_1(2^{31})^1 + \dots m_n(2^{31})^n$

- 2) Converting each coefficient  $m_n$  of the  $2^{31}$  series obtained in step 1, above, into a binary series

Coefficients of the individual numbers in the  $2^{31}$  series obtained from the above step are converted into a series of power of 2. A function is used to convert each coefficient into a series of powers of 2.

- 3) To optimize the searching process, a proprietary method is used that comprises the following steps and uses a lookup table.

- i) Computing the SIZE = size of  $N$  (in digits), where  $N$  is a number
- ii) computing  $POINTER = 3 \cdot (SIZE) + INT(SIZE/3) - 4$

Thus, by computing the pointer, the search process is optimized.

The Ye publication does not disclose the claimed scalar multiplication as set forth in independent claim 12 and further defined dependent claims 16 and 17. It is settled law that "[a] claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Brothers Inc. v. Union Oil Co. of California*, 2 USPQ2d, 1051, 1053 (Fed. Cir. 1987). In light of the aforementioned arguments made with respect to the anticipation rejections under the Ye publication, whose underlying anticipation teachings, now refuted, are used for rejecting claims 12-21 on an obviousness basis in view of the teachings of the SEC article, Applicants hereby respectfully request that the Examiner withdraw the overall obviousness rejection of independent claim 12 and the claims depending therefrom.

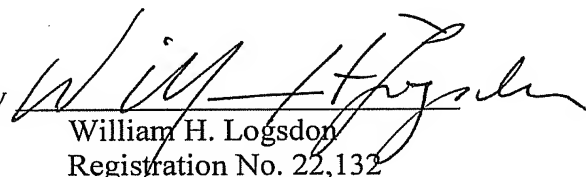
### CONCLUSION

Based on the foregoing amendments and remarks, reconsideration of the rejections and allowance of pending claims 12-19 are respectfully requested.

Respectfully submitted,

THE WEBB LAW FIRM

By



William H. Logsdon  
Registration No. 22,132  
Attorney for Applicants  
700 Koppers Building  
436 Seventh Avenue  
Pittsburgh, PA 15219  
Telephone: 412-471-8815  
Facsimile: 412-471-4094  
E-mail: [webblaw@webblaw.com](mailto:webblaw@webblaw.com)